ISC14D009

Title:	***Information Classification and Data Management policy review***
Author:	Raymond Scott (ISD)
Date:	22 January 2015
Circulation:	ISSC 16 February 2015
Agenda:	ISC14A002
Version:	Draft v2.2
Status:	Open

Issue

To seek the committee's approval for proposed changes to the Information Classification and Data Management policy.

Recommendation

Recipients are invited:

- To approve the revised policy

Resource implications

No change to service is required and therefore there is no impact on resources.

Risk implications

The local policy is offered to help the University identify material which should be secured and handle it appropriately, particularly personal data which must be handled in accordance with the Data Protection Act 1998. The proposed changes are made to help reduce the risk of non-compliance and to make the policy more accessible.

Equality and diversity

New services will be subject to Equality Impact Assessment as they are implemented.

Timing of decisions

Once approval is obtained the revised policy can be put into effect and published.

Further information

- Raymond Scott (ISD), x3651 r.scott@uea.ac.uk

Background

The policy is subject to annual review. This paper contains the updated policy for which a summary of the specific and general changes are listed below.

Discussion

The following changes are have been made to the document:

- The document has been simplified by the removal of some repeated information.
- The previous set of information classes has been compared against the Committee Office's current practice for the classification of committee papers, and the Government Security Classification scheme[1] which came into force on 2 April 2014. As a result of this, the 'Internal' class has been removed.
- It should be noted that the removal of the 'Internal' class does not mean that there is no need for intranet web facilities. Material put onto the intranet will have a security class of 'Open' and be available to the whole UEA community. If the material needs to be secured against unauthorised access, it will have a secure classification (confidential or secret) and will not be stored on the web.
- In general, we aim for policy documents just to contain policy statements, and for supporting guidance on the application of the policy to be held on web pages linked to from the policy. In this spirit, we have removed the guidance on the selection of third party cloud storage tools for particular purposes and moved it onto the web site.
- The policy has been updated to account for the provision of OneDrive for Business – UEA's new cloud-based collaboration environment providing tools and storage – provided as part of our migration to Office 365.

Attachments

- Information Classification and Data Management policy v2.2 DRAFT

[1] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251480/Government-Security-Classifications-April-2014.pdf

Information Classification and Data Management policy

Report Control Information

Title:	Information Classification and Data Management Policy
Date:	16 January 2015
Version:	2.2 (Approved by ISSC XXXXX)
Authors:	ISD SPC
Quality Assurance:	ISSC
Security class	Open

Revision	Date	Revision Description
v.1.0	17/7/07	As approved by ISSC
v.1.2	9/5/11	Reviewed and approved by ISSC June 2011. Revisions as part of Security Review project and based on recommendations following external consultant's report.
v.1.3	14/5/11	Updated for review by IT Forum 21/5/12 and ISSC 12/6/12
v.2.0	12/6/12	As approved by ISSC
v.2.2	16/1/15	Reviewed and updated (removed Internal class and renamed Public to Open)

Definitions of terms

Information Asset	An information asset is a collection of any type of data, irrespective of type (e.g. numerical data, text) and format.
Data Owner	The Data Owner is the person or department within UEA who has overall responsibility for the information asset and for ensuring that it is managed securely and in compliance with University and government regulations and policies. The Data Owner may delegate day-to-day responsibility for management of the data to a Data Administrator, service group or other persons.
Data Administrator	The Data Administrator is the UEA staff member or department delegated with overall responsibility for day to day management of the information asset in accordance with University and government regulations and policies. Processes and procedures used to manage the data should have been agreed with the Data Owner. For some data, particularly small datasets, the Data Owner and Data Administrator may be the same person.
Security class	Defines how an information asset should be handled. The classes are: Open, Confidential and Secret.
Data management plan	A document which describes how you will handle the data associated with a project, both during its lifetime and after it has completed.
Information asset register	A document listing your information assets and key metadata about them: owner, administrator, location, user access, retention policy, and information class.

Objective

The objective of this policy is to provide a classification system for all University data and documents (**information assets**) to which an appropriate **security class** can be assigned.

The University holds many information assets that must be protected against unauthorized access, disclosure, modification, or other misuse. Efficient management of these assets is also necessary in order to comply with legal obligations under the Data Protection Act, the Freedom of Information Act and Environmental Information Regulations.

Different types of information assets require different security measures. Proper classification is vital to ensuring effective data security and management. Each security class listed in the summary tables below has defined data management controls which determine how information assets should be handled throughout its lifecycle. These controls should be applied to all information assets held by the University.

Scope

This policy is to be applied to all information held by the University, including data and documents relating to UEA teaching, research and administration. The focus of the policy is on information held in an electronic format, however departments should also apply appropriate controls to information held in hard copy. The policy encompasses storage, access, sharing and resilience of information assets.

Responsibility

Data Owners and **Data Administrators** are responsible for identifying the appropriate security class for any information assets within their care and ensuring that the appropriate data management policies governing storage, dissemination, disposal etc. are followed.

Where information is classified not for public consumption (i.e. Confidential or Secret) this should be made clear to those who have access to the data. If management of such data is delegated to other individuals, the Data Owner and Data Administrator must ensure that appropriate guidance is provided.

Data Owners and Administrators are responsible for ensuring that information assets are processed and managed in accordance with UEA's Records Management policies as detailed at: https://www.uea.ac.uk/is/strategies/infregs/Records+management.

Incident management

Where data has been incorrectly classified, or has not been managed in accordance with its security class, this should be reported immediately to the Strategy, Policy and Compliance team who will log the incident and refer it to the service team, Data Administrator or Data Owner as appropriate for them to action.

Audit and accountability

All projects and services with significant handling of data should have a documented **data management plan/information asset register** describing the data to be used, the Security Classes assigned to these categories of data, the identity of the data owners and the data management policies to be applied. The plan/register should be made available on request to those authorised by the University to carry out security or data protection audits (contact ISD Information Policy and Compliance Managers for details).

Implementation

At the point of creation, all University data will be classified and handled in accordance with the following tables of Information Classes and Data Management Policies. By default, all data are classed Open (accessible to the world). One of the other security classes is applied to data which must be protected.

Summary tables of Information Classes and Data Management

Security class	OPEN
Description	Public information relating to the University. E.g. programme and course information on UEA's web pages, press releases, published research papers
Storage	Stored on centrally managed facilities backed up on a 24hr basis, e.g. centrally managed filestore, UEA Office 365 OneDrive for Business and UEA web pages including intranet pages[2]. Or Appropriate third party storage[3]
Dissemination and access	• Widely available • Unrestricted dissemination via electronic or hard copy • Dissemination must not violate any applicable laws or regulations. • Information should be identifiable as from • UEA • Permissions to modify limited to authorised persons and procedures in place to ensure that information is kept up to date.
Transmission or collaboration	Via web, email, appropriate third party storage or printed copy
Security impact[4]	Negligible
Example security measures[5]	• Stored on UEA Content Management System (CMS) and public-facing web pages • Stored on author's centrally managed filestore • Stored on OneDrive for Business • Stored on departmental central filestore share with write permissions restricted to authorised individuals
Disposal	• Electronic data deleted using normal file deletion processes • Printed material disposed of via non-confidential recycled waste, i.e. does not require shredding or disposal in 'blue bins'

[2] You may choose to put Open documents on the intranet if they do not need to be secured, but you want to limit access only to UEA staff and students for some other reason.
[3] See separate guidance
[4] The likely impact on the University's business and reputation if appropriate security controls and data management were not applied and unauthorised persons were to gain access to the information.
[5] The listed example security measures are not exhaustive and other methods of securing data may be appropriate. Contact isd.spc@uea.ac.uk for advice.

Security class	CONFIDENTIAL
Description	• Information restricted to members of UEA, partner organisations and other individuals, as authorised by Data Owners • Information may be restricted to a specific subset of the University including a restricted set of non-University members • Information which is sensitive or contains personal information relating to individuals. E.g. employee information such as payroll, exam papers, exam marks, notes relating to disciplinary processes, research data containing personal information or information which is of a high value.
Storage	Stored on centrally managed facilities backed up on a 24hr basis with access restricted to authorised individuals, e.g. centrally managed filestore, UEA Office 365 OneDrive for Business Or Appropriate third party storage
Dissemination and access	• Dissemination limited to authorised personnel only • Where restricted to a particular group, only authorised personnel allowed to have access to the information
Transmission or collaboration	• May only be transmitted outside institution systems in encrypted format • Any distributed documents (electronic or paper) to be marked as 'Confidential' and the intended recipients clearly indicated • Printed copies to be delivered by hand directly to the recipient. Use of shared folders on centrally managed facilities, for collaboration with external parties use OneDrive for Business or a UEA account with VPN access • Appropriate 3rd party storage can be used provided encryption /appropriate security controls are in place
Security impact	Medium to high
Example security measures	• Stored on centrally managed filestore with access control mechanisms applied • Stored on OneDrive for Business • In exceptional circumstances where information is stored on portable electronic storage devices or media, that storage to be encrypted • Printed copies kept secure, e.g. in locked filing cabinet with only authorised individuals having access
Disposal	On decommissioning of equipment used to store the data, the storage should be securely wiped to CESG Enhanced standard[6], or physically destroyed. Printed copies to be shredded.

[6] CESG Enhanced standard - UK Communications Electronics Security Group (CESG) Enhanced standards

Security class	SECRET
Description	Any confidential information which can have a major impact on the long-term viability of the University.
Storage	Stored on centrally provided special facilities or UEA Office 365 OneDrive for Business in an encrypted format. Or Appropriate third party storage
Dissemination and access	Dissemination and access strictly controlled by the Data Owner, limited to very few authorised individuals and all access logged.
Transmission or collaboration	• Not normally transmitted via email, but where this is essential both the transmission and the content must be encrypted • Shared folders on centrally managed facilities and OneDrive for Business can be used • Appropriate 3rd party storage can be used provided encryption/appropriate security controls are in place. Data owners are advised to seek advice from ISD in advance of using third party storage for this data class
Security impact	Very high
Example security measures	• Stored on special area of central filestore to which only the Data Owner has access and only they can allow access to other authorised individuals • Document access limited at all times by encryption keys
Disposal	As for Confidential class.